(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 January 2002 (17.01.2002)

PCT

(10) International Publication Number
WO 02/05478 A1

(51) International Patent Classification[7]: H04L 9/00

(21) International Application Number: PCT/US01/21038

(22) International Filing Date: 5 July 2001 (05.07.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/217,151 9 July 2000 (09.07.2000) US

(71) Applicant and
(72) Inventor: **BLACK, Gerald, R.** [US/US]; 30590 Southfield Road #160, Southfield, MI 48076 (US).

(74) Agent: **BLACK, Gerald, R.**; 30590 Southfield Road #160, Southfield, MI 48076 (US).

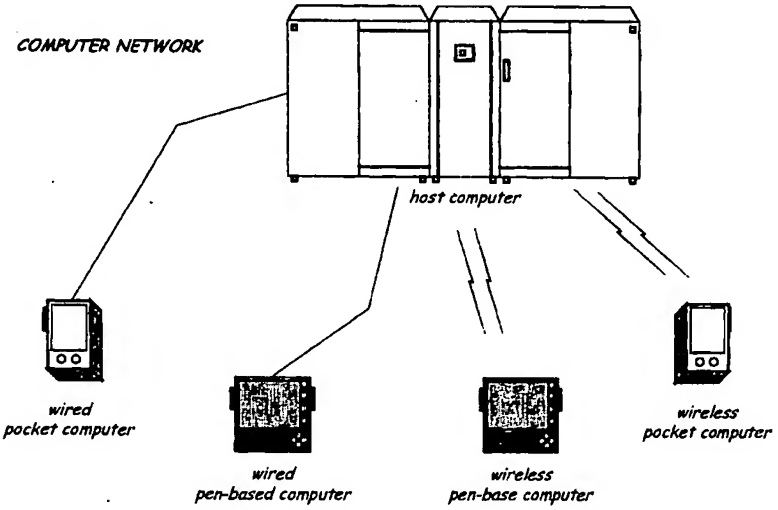
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: NETWORK SECURITY SYSTEM



(57) Abstract: A network security system comprises a host computer, and a plurality of remote computers. Each computer provides fingerprint authentication of a user prior to responding to the user request for data access. The remote computers are handheld when in operational mode. A sensor in the computer housing captures a print of a finger or hand of the user while the remote computer is being held. The fingerprint sensor is positioned in such a way that the sensor remains in continual contact with the hand of the user while the remote computer is being held by the user enabling a continual authentication of the identity of the user with each request for access to each secure record. The fingerprint authentication is captured in an incidental manner as the data request is submitted from the remote computer to the host computer enabling user identity authentication simultaneously with each request to access the secure record.

WO 02/05478 A1

NETWORK SECURITY SYSTEM

FIELD OF USE

The present invention relates to a network security system with identity authentication, and more particularly, to such authentication by biometric capture as access to data from a remote computer to a host computer is being processed.

BACKGROUND OF THE INVENTION

The global workforce is increasingly mobile and handheld computing is on the rise. Smart handheld processors are emerging from the realm of individual purchases to enterprise deployment as they become key tools for connectivity to the corporate environment. Development of handheld applications and wireless technology tailored for a specific enterprise represent are serving the increasing mobile worker population. Handheld computer systems are ideal for applications which require: (1) highly portable devices - that are no longer constrained by a keyboard; (2) intuitive features - that resemble an environment familiar to the users; (3) improved efficiency, - that enables accurate data collection and manipulation; and (4) flexibility - that enables a wide variety of types of data entry.

By the year 2005 as much as 50 percent of all communication terminals will be mobile. These machines, while offering substantial storage capacity and computing power have only limited communication capabilities. As a result, users are gaining access to the powerful computing infrastructure.

Security is no longer an optional network component. Today organizations of all sizes are discovering the need to protect their networks from both external and internal unauthorized users. In the days before remote access, organizations had controlled, hard-wired networks, which provided a certain degree of physical security. Network access was limited to users physically located in the building. Requiring users to type in a name and password, added another layer of security to the network. Providing remote network access has added an entirely new dimension to network access and system integrity.

U.S. Patent No. 5,838,306 (O'Connor, et al.) discloses a mouse with a security feature. The mouse computer input peripheral device includes a window area integrally constructed within the mouse and positioned at an area on the mouse upon which a user normally places a finger in operating the mouse. U.S. Patent No. 5,991,413 (Borza, et al.) discloses a mouse adapted to scan fingerprint data. In an attempt to address these concerns, a biometric pointing device such as a mouse is presented incorporating therein a contact imager. The contact imager fits within a small enclosure. Further, data transmission means within the mouse provides a signal to a single port on a computer indicative of the output data from both the contact imaging means and the pointing device. Also, PCT Application No. PCT/US99/17900 entitled "Identification Confirmation System" filed on April 7, 1999; U.S. Patent Application 09/490,687, entitled "Writing Implement and Network security systems" filed on January 24, 2000; U.S. Patent Application 09/535,411, entitled "Method for Identity Verification" filed on March 20, 2000; and PCT Application No. PCT/US00/19652 entitled "Identity Authentication System and Method" filed July 18, 2000 by this applicant disclose the use of fingerprint sensors disposed in the barrel of a stylus used to generate an electronic signature as the preferred digital signature.

In addition, Polaroid has introduced a low-cost finger image scanner, targeting users with concerns for desktop security concerns and for personal security in e-commerce. The new finger image scanner is built into keyboards. Compaq Computer also markets a keypad with a fingerprint scanner.

While connected to systems and retrieving or transmitting data, security is at times critical. Secure connections may not be necessary when browsing the news, for example, but are desirable when connected to corporate databases or when electronic commerce is undertaken.

What is needed is a network security system wherein data resources are available only to authorized users and when requested, confidential information is available only to authorized parties, the user's identity is continually authenticated, and the user cannot deny the communication. What is needed is a network security system that authenticates identity for access to secure networks; that authenticates in a

nonobtrusive manner with each data access request without the necessity of extra hand or finger movements that are distracting; that authenticates continually to ensure that the person seeking data access has been authorized for such access; and that is secure and discourages hackers.

SUMMARY OF THE INVENTION

The network security system of the present invention addresses these needs and dramatically improves the nature data access for handheld computers. The preferred embodiment of the network security system of the present invention comprises a host computer, and a plurality of handheld computers. Each computer provides advanced biometric authentication of a user prior to responding to the user request for data access. The handheld computers are handheld when in operational mode. A sensor in the computer housing captures a print of a finger or hand of the user while the computer is being held. The biometric sensor is positioned in such a way that the sensor remains in continual contact with the hand of the user enabling a continual authentication of the identity of the user with each request for access to a secure record. The biometric sensor is preferably a fingerprint sensor. The fingerprint authentication is captured in an incidental manner as the data request is submitted from the handheld computer to the host computer enabling user identity authentication simultaneously with each request to access the secure record.

Each computer of the present invention in the network security system of the present invention is a handheld processor that enables access to a computer network and a biometric sensor disposed in the casing of the handheld processor. These handheld processors maintain continual contact with a finger, thumb, or palm of the user so that biometric authentication can be accomplished without the need to press special surfaces or otherwise alter conventional computer manipulations. While the technology of the present invention applies to all portable computers (e.g. - laptops, handhelds, palms, and pockets), the technology is preferably directed at palm and pocket computers.

In the network security system of the present invention, a palm or pocket computer the size of the user's hand is used that can conveniently be held in one hand. One or more fingerprint sensors are disposed in the back or side surfaces of the handheld computer

such that the identity of the user is continually verified while the computer is being held and used. The ability to provide continual verification by means of biometric print sensors is particularly important to ensure network security.

While fingerprints and palm prints are used in this application for purposes of illustration, it is understood that the principles of this invention are also applicable to other biometric technologies where identity can be confirmed when the user touches a sensor, such as cell capture and DNA.

For purposes herein, a list of key terms is hereafter set forth to clarify the scope of this specification. A "handheld computer" refers to any computing device and application, including, but not limited to, a pocket computer; a palm-type computer; a laptop computer; a cell-phone; and similar devices, that involve continual contact with the hand of the user during routine usage. Also, many smaller computers are embedded in walls, desktop, and car instrument panels, and are generally precluded from these definitions unless the user continually touches a part of such computers. A "remote computer" refers to a hard-wired or wireless handheld computer. "Casing" refers to either the housing of the handheld computer or a pocket or container for storing the handheld computer.

"Biometrics" refers to the technology of verifying the identity of an individual by measuring and analyzing data relative to a physiological characteristic or behavioral characteristic of an individual. Examples of physiological characteristics are retina, iris, hand geometry, body odor, and fingerprint; and examples of behavioral biometrics are voice, keystroke rhythm and signature. A "fingerprint" is a biometric and refers to either the print of the thumb, index finger, any other finger, or combination thereof.

For a more complete understanding of the network security system of the present invention, reference is made to the following detailed description and accompanying drawings in which the presently preferred embodiments of the invention are shown by way of example. As the invention may be embodied in many forms without departing from spirit of essential characteristics thereof, it is expressly understood that the drawings are for purposes of illustration and description only, and are not intended as a

definition of the limits of the invention. Throughout the description, like reference numbers refer to the same component throughout the several views.

BRIEF DESCRIPTION OF THE DRAWINGS

FIGURE 1 is a schematic the preferred embodiment of the network system of the present invention;

FIGURE 2A shows a view of the backside of a palm computer for use in the network security system of FIGURE 1, the palm computer having a pair of fingerprint sensors capturing print of the thumb and index finger of the user and a third sensor to capture the palm print of the user, for identity authentication while the palm computer is being used, and FIGURE 2B shows the frontside of the palm computer of FIGURE 2A;

FIGURE 3 discloses the frontside of another processor device for use in the network security system of FIGURE 1, a fingerprint sensor being positioned in the casing of a palm computer;

FIGURE 4 discloses yet another processor device for use in the network security system of FIGURE 1, the processor device being a full screen computer, the processor device having a fingerprint sensor disposed on a side of the full-screen computer;

FIGURE 5 discloses a simplified logic diagram of one embodiment for registering in the network security system of FIGURE 1, a user file and reference biometrics being secured in a user file that is created during the registration process;

FIGURE 6 discloses a simplified logic diagram of one embodiment for logging onto the network security system of FIGURE 1, a captured print being compared to a reference record for purposes of authentication;

FIGURES 7A and 7B disclose a simplified logic diagram of one preferred embodiment for requesting access to the network security system of the present invention;

FIGURES 8A and 8B disclose a simplified logic diagram of one preferred embodiment for

requesting entry of new data to the network security system of the present invention;

FIGURES 9A and 9B disclose a simplified logic diagram of one preferred embodiment for requesting access to high security data of the network security system of the present invention, the high security data access request requiring a match authentication of a pair of user fingerprints;

FIGURE 10A discloses a simplified layout for a user record of one preferred embodiment of the network security system of the present invention;

FIGURE 10B discloses a simplified layout for a data access record of the preferred embodiment of the network security system of FIGURE 10A;

FIGURE 10C discloses a simplified layout for a remote processor record of the preferred embodiment of the network security system of FIGURE 10A;

FIGURE 11 discloses a simplified flowchart for performing a network security audit of the network security system of the present invention;

FIGURE 12A discloses a simplified curve analysis for a regular security environment where the threshold position is located at the juncture of the normal curve for authorized users and the normal curve for unauthorized users; and

FIGURE 12B discloses a simplified curve analysis showing for high-security applications similar to FIGURE 12A, where the position of the threshold has been repositioned to minimize false negatives.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Referring now to the drawings, FIGURE 1 discloses the preferred embodiment of the network security system of the present invention. The preferred embodiment of the network security system of the present invention comprises a host computer, and a plurality of handheld computers. Each handheld computer provides authentication of a

user prior to responding to the user request for data access. A sensor of a biometric property of the user disposed in the computer housing captures a biometric print of the user while the handheld computer is being held. The biometric sensor is preferably a fingerprint sensor.

As shown in FIGURE 2A and 2B, at least one fingerprint sensor is positioned at one or more strategic sites such that a portion of the hand of the user is in continuous contact therewith during usage of the processor, enabling a continual authentication of the identity of the user with each request for access to each secure record. The fingerprint authentication is captured in an incidental manner as the data request is submitted from the handheld computer to the host computer enabling user identity authentication simultaneously with each request to access the secure record. As shown, the processor includes sensors to capture a thumbprint, the print of the index finger, and a palm print. Also, a palm print sensor can be disposed on the back surface of the computing device of the present invention to supplement or complement the fingerprint sensors. Multiple sensors are recommended for high-security applications (see for example FIGURES 9A and 9B).

FIGURE 3 discloses the frontside of another embodiment of a processor device for use in another preferred embodiment of the network security system of the present invention. The fingerprint sensor is positioned in the casing of a palm computer, the casing being used to house the palm computer when used and stored. The casing may also be a wallet or pouch in digital engagement with the processor, either through wire or a wireless mode - enabling identity authentication whenever network access to data is required. The principle advantage of this approach is that registration is conducted through the casing and the computers need not be altered (off the shelf).

FIGURE 4 discloses yet another full-screen processor for use in the network security system of the present invention. These processors are sometimes referred to as handheld computers in the literature, but are referred to as full-screen processors herein for clarity. The screen is roughly the size of a screen of a PC, except that the computer does not have a conventional keypad. A fingerprint sensor is disposed on one side of the full-screen computer.

The strategic positioning of individual and multiple sensors depends on the size and shape of the individual computer, and the size of the hands of the computer user. And, it is advised that either the location of the sensors is symmetrical (both sides of the processor) to accommodate both left-handed and right-handed users. Alternatively, some processors can be designed for right-handed users and others for left-handed users.

Referring now to FIGURE 6, the user enrolls his or her prints by submitting the thumb, index finger, and/or palm prints to the network in a secure process. The reference print is preferably stored in the host computer for security purposes to prevent user access and tampering. The prints may need to be stored in the system also. Subsequently, when network access is requested, the relevant print or prints are captured and compared against the reference prints. Only upon authentication is network access enabled to authorized users. Data access is only enabled once a match has occurred that equals or exceeds a threshold value that has been set in accordance with the sensitivity of the data being requested access to. The system also enables varying levels of security within the same network since person A may be permitted access to certain data, and person B permitted access to other data. For example both are permitted access to general network data, but each is only permitted access to his/her own personal or employment or medical files.

For most lower security applications, one sensor is adequate. However, in many higher security applications, multiple prints may be appropriate, since processing occurs based upon only a partial print. The network security system of the present invention enables system designers to integrate into the system the level of security needed for each application, while allowing improved security to be incorporated as needed.

The network security system of the present invention continually controls network access and ensures the integrity of all data. The system enhances security without the need to modify the casing of the computer with card-readers or sensing devices. Identity is authenticated continually and routinely, each time there's a request to access additional information.

The preferred embodiments of the network security system of the present invention requires authentication prior to each login; each request for data access; and each data entry. FIGURE 6 discloses a simplified logic diagram of one embodiment for logging onto the network security system of the present invention. A captured print is compared to a reference record for purposes of authentication. Since the network may include data that is not confidential (like Internet access), the user need only be authorized to access the handheld computer to gain system access - this is not recommended for high security networks.

The preferred embodiments of the network security system of the present invention create a fingerprint-authenticated record of each user (data access and entry); of each record; and of each computer. FIGURES 7A and 7B disclose a simplified logic diagram of one preferred embodiment for requesting access to the network security system of the present invention. Similarly, FIGURES 8A and 8B disclose a simplified logic diagram of one preferred embodiment for requesting entry of new data to the network security system of the present invention.

FIGURES 9A and 9B disclose a simplified logic diagram of one preferred embodiment for requesting access to high security data of the network security system of the present invention, the high security data access request requiring a match authentication of a pair of user fingerprints. The handheld computer of FIGURE 2A and 2B enable the capture of multiple fingerprints.

FIGURE 10A disclose a simplified layout for a user record of one preferred embodiment of the network security system of the present invention. FIGURE 10B discloses a simplified layout for a data access record of the preferred embodiment of the network security system of FIGURE 10A. FIGURE 10C discloses a simplified layout for a remote processor record of the preferred embodiment of the network security system of FIGURE 10A.

FIGURE 10A depicts a simplified user record for the network security system of the present invention. The user record includes the user's name, address, reference prints and signature, user authorized security level, a list of data records that the user is authorized to access, a list of handheld computers that the user is authorized to use, a history of records accessed by the user, and a list of records that the user was denied

access to and when. FIGURE 10B depicts a simplified data record for the network security system of the present invention. The data record includes a data record number, a data security level, names of users authorized to access this record, the reference prints of authorized users, a list of handheld computers authorized to access this record, a history of persons who accessed this record and when, and a history of all persons denied access to this record. FIGURE 10C depicts a simplified computer record for the network security system of the present invention. The computer record includes a remote computer number, the names of authorized users, the reference prints of all authorized users, a list of records that can be authorized from this computer, a list of all persons authorized to access each record, a history of all persons using this computer, a history of all users denied access to the computer, and prints of all users denied access to the computer. Each of these records is updated upon the occurrence of each relevant user, record, and computer event to enable a tracking for audit purposes.

FIGURE 11 discloses a simplified flowchart for performing a network security audit of the network security system of the present invention. Routines investigation as to network activity is needed to identify and remedy any security breaches. For these purposes, a distinction is made between an authorized attempt to enter a record or computer and an incidental breach - the latter being the result of sensor error or innocent mistakes by a user during network usage.

FIGURE 12A discloses a simplified curve analysis for a regular security environment where the threshold position is located at the juncture of the normal curve for authorized users and the normal curve for unauthorized users. By placing the threshold at such juncture, there will be considerably more false positives (an authorized user denied entry) than false negatives (an authorized user gaining entry) - and this is generally an acceptable balance of the competing interests. FIGURE 12B discloses a simplified curve analysis showing for high-security applications where the position of the threshold as shown in FIGURE 12A has been repositioned to minimize false negatives. In these high-security applications, essentially any unauthorized entry is unacceptable and so the threshold is reduced - resulting in an increase in false positives.

Several applications of the network security system of the present invention include:

Nurses and doctors can track and record patient histories as they make their rounds, using clipboard-like computers and pens to access and enter patient information over a wireless network from servers throughout the hospital. Insurance claims adjusters can assess automobile damages on site, looking up relevant cost information with the handheld computer, then printing the estimate and writing a check to the repair shop at the end of the visit.

Sales representatives can track inventory and the effect of promotional campaigns in retail stores, using a pen-based computer. At the end of the day, the information is transmitted through a phone line back to headquarters.

Government employees in the field or traveling on business can access secure data, with authentication and assurance that the person is the remote user authorized to access each data stream.

Inkless fingerprint sensors have now been developed that capture a forensic quality fingerprint in less than a second. The fingerprint sensors packages are less than 0.75 in. wide, and smaller packages are being developed. Infineon (associated with Siemens) and STMicroelectronics (formerly SGS Thomson) manufacture the sensors of choice.

The Infineon sensor enables the integration of a miniature fingerprint sensor into a wide variety of end products. The chip is compact, and robust enough to convert a previously exotic technology-biometric user ID into an everyday reality. The chip is a small (18mm x 21mm x 1.5mm) IC embedding a 288 x 224 pixel contact sensor array that images the lines and ridges of a human fingerprint when a user touches the device. Each pixel has an 8-bit data depth, enabling evaluation of subtle gradations (256 shades of gray) of a fingertip and their translation into a set of indices - the key identifying features of an individual fingerprint. Imaging and data transfer of an impression takes 100 milliseconds. The STMicroelectronics fingerprint sensor is substantially the same size as the Infineon sensor and that use capacitive-sensor-array technology, building silicon IC's containing an array of sensor plates. ST technology uses a capacitive sensing technique to capture, in less than one tenth of a second, a high-resolution image of a fingerprint when the finger is applied directly to the chip surface. The output of the chip is a digital representation

of the fingerprint, which can be processed by the algorithms developed by SAGEM, which immediately confirm or invalidate the recognition of pre-identified persons and then be further processed by application-dependent software.

Another biometric that is recommended in the network security system of the present invention involves cell capture while the processor device of the present invention is being used. The advantage of this biometric over fingerprints is that accuracy is not dependent upon the size of the sensor or print that is captured.

GeneTrace Systems has a high-resolution mass spectrometry-based method for chemical analysis of large single-stranded DNA oligomers. The mass spectra are obtained in seconds instead of the usual hours needed for gel electrophoresis currently used, and no radioactive or fluorescent materials are needed. The technique has high mass capabilities and opens new avenues of study as in chemical modifications of DNA, DNA-peptide/protein interactions such as antisense drug development. DNA sequencing and quality control for synthetic DNA and related products are also potential applications. The basic technology can be applied also to peptides and proteins and used for protein structure determination, phosphorylation, glycosylation, and other studies. Previously it had not been possible to apply mass spectrometry successfully to anything larger than about a 4-mer and thereby obtain the advantages the mass spectrometry technique can offer in precise and accurate molecular weight determination. The new physico-chemical sample preparation opens this capability to single-stranded DNA molecules above 50,000 Dalton with a mass accuracy of 0.01 percent in the 10,000 Dalton range. This is much higher accuracy and resolution than is obtainable with state-of-the-art electrophoresis techniques.

Another approach is to use surface-confined arrays of highly selective sensing elements. Chemical and biological sensors are required to perform multi-analyte measurements rapidly, accurately, and at increasingly lower cost. Arrays of immobilized single-stranded DNA (ssDNA) probes, so-called DNA chips, are being used for genetic analysis for disease detection, toxicology, forensics, industrial processing, and environmental monitoring.

The network security system of the present invention provides network access security by; (1) controlling unauthorized access to the network; (2) controlling improper access by

network users; and (3) monitoring user access to network resources. The network security system of the present invention initially identifies the user, and continually controls and monitors user activity while the user is plugged in.

When wireless devices are used, system security becomes more of a concern, since an integral part of the system, in this instance the wireless computers, are not attached to the system, but rather are portable and carried by a customer. A preferred method of authenticating a remote computer is to make each remote computer unique from all others. The unique quality is identified and stored in the host computer. A comparison is made between the unique quality of the remote computer and the stored value in the host computer prior to enabling access to or entry of a data stream. This can be done with the random use photo refracted crystals as shown in U.S. Patent No. 5,619,025 (Hickman, et al.); at least two magnetic filaments or strips and preferably includes a multiple number of filaments of differing coerciveness, magnetic field strength, magnetic field alignment, size or spacing so that when the remote computer requests data access, approval will be given only when the proper signal is provided by the ordered array of appropriate magnetic elements in the wireless computer as shown in U.S. Patent No. 5,834,748 (Litman)

Throughout this application, various Patents and Applications are referenced by patent number and inventor. The disclosures of these Patents and Applications in their entireties are hereby incorporated by reference into this specification in order to more fully describe the state of the art to which this invention pertains.

It is evident that many alternatives, modifications, and variations of the network security system of the present invention will be apparent to those skilled in the art in light of the disclosure herein. It is intended that the metes and bounds of the present invention be determined by the appended claims rather than by the language of the above specification, and that all such alternatives, modifications, and variations which form a conjointly cooperative equivalent are intended to be included within the spirit and scope of these claims.

CLAIMS

1. A computer network comprising:

a host computer; and

a plurality of remote computers, each remote computer being distal from the host computer, a remote computer providing authentication of a user prior to responding to the user request, the authentication being fingerprint authentication, the fingerprint authentication being captured continually, the fingerprint authentication being captured in an incidental manner as the data request is submitted from the remote computer to the host computer enabling user identity authentication simultaneously with the request to access the secure record.

2. A computer network comprising:

a host computer; and

a plurality of remote computers, each remote computer being distal from the host computer, a remote computer providing authentication of a user prior to responding to the user request, the authentication being biometric authentication, the fingerprint authentication being captured continually, a biometric property being captured in an incidental manner as the data request is submitted from the remote computer to the host computer enabling user identity authentication simultaneously with the request to access the secure record.

3. A system for restricting data access of a computer user to a data network, the system comprising:

a remote processor having access to a computer network through a digital connection with a host computer, the remote computer being remote from the host computer, the remote computer being handheld while in operational mode, the remote computer having a casing; and

a sensor disposed in the remote computer, the sensor providing user authentication by capture of a predetermined characteristic of the computer user and comparison of the sensed predetermined characteristic with a reference predetermined characteristic, the capture occurring while the remote computer is being held by the computer user, the sensor being disposed in part of the remote computer that is touched by a portion of the hand of the computer user while the remote computer is being used, the sensor enabling a capture of the predetermined characteristic in an incidental manner as the request for data access is being processed.

4. A system for restricting data access of a computer user to a data network, the system comprising:

a remote computer having access to a computer network through a digital connection with a host computer, the remote computer being remote from the host computer, the remote computer being handheld while in operational mode, the remote computer having a casing; and

a sensor disposed in the remote computer, the sensor providing user authentication by capture of a predetermined characteristic of the computer user and comparison of the sensed predetermined characteristic with a reference predetermined characteristic, the capture occurring while the remote computer is held by the computer user, the sensor being disposed in the casing of the remote computer that is touched by at least a portion of the hand of the computer user while the remote computer is being used, the sensor enabling a repeated capture of the predetermined characteristic in a continual manner while the remote computer is being held.

5. A system comprising:

a remote computer access to a computer network, the remote computer being portable, the device being handheld when in operational mode; and

a biometric sensor disposed in the casing of the remote computer, the sensor enabling capture of a finger or hand of the user while the remote computer is being

held, the biometric sensor being positioned in such a way that the sensor remains in continual contact with a portion of the hand of the user while the remote computer is being used enabling a continual verification of the identity of the user during access to the computer network.

6. A method for restricting data access to a computer user relative to a data network through a remote computer, the remote computer being remote from a host computer, the method comprising:

holding at least a portion of the remote computer with at least a portion of the hand of the computer user;

requesting a login to the data network through the remote computer;

sensing a predetermined characteristic of the user making the request, the remote computer being handheld when in operational mode, the sensing being accomplished by use of a sensor, the sensor being disposed in the portion of the remote computer that is touched by a portion of a hand of the computer user during computer usage, the sensing being accomplished in an incidental manner while the computer user holds the remote computer and requests access to additional data-streams;

comparing the sensed predetermined characteristic of the computer user with a reference predetermined characteristic; and

providing network access representative of the comparing the sensed predetermined characteristic and the reference predetermined characteristic.

7. A method for restricting data access to a user relative to a data network through a remote computer, the remote computer being remote from a host computer, the method comprising:

holding at least a portion of the remote computer with at least a portion of the hand of the computer user;

requesting a login to the data network through the remote computer;

sensing a predetermined characteristic of the user making the request, the remote computer being handheld when in operational mode, the sensing being accomplished by use of a sensor, the sensor being disposed in the portion of the remote computer that is touched by a portion of the hand of the computer user during computer usage, the sensing being accomplished continually while the computer user holds the remote computer and requests access to additional data-streams;

comparing the sensed predetermined characteristic of the computer user with a reference predetermined characteristic; and

providing network access representative of the comparing the sensed predetermined characteristic and the reference predetermined characteristic.

8. A method of enabling access to a computer network, the method comprising:

logging onto a remote computer, the remote computer being touched by a portion of a hand of a user during computer usage;

capturing a first biometric identifier of a user while the remote computer is being held relative to such holding; and

enabling access to the computer network when the captured biometric matches a reference biometric, and blocking access to the computer network in the absence of a match between the captured biometric and the reference biometric.

9. A casing for a remote computer, the casing comprising:

a pocket for housing the remote computer, the remote computer enabling access to a computer network, the remote computer being touched by a portion of a hand of a user during computer usage; and

a biometric sensor disposed in the outer surface of the casing, the biometric sensor

enabling capture of a biometric property from the hand of the user while the remote computer is being held, the biometric sensor being positioned in such a way that the sensor remains in continual contact with the hand of the user while the remote computer is being held by the user enabling a continual verification of the identity of the user during access to the computer network.

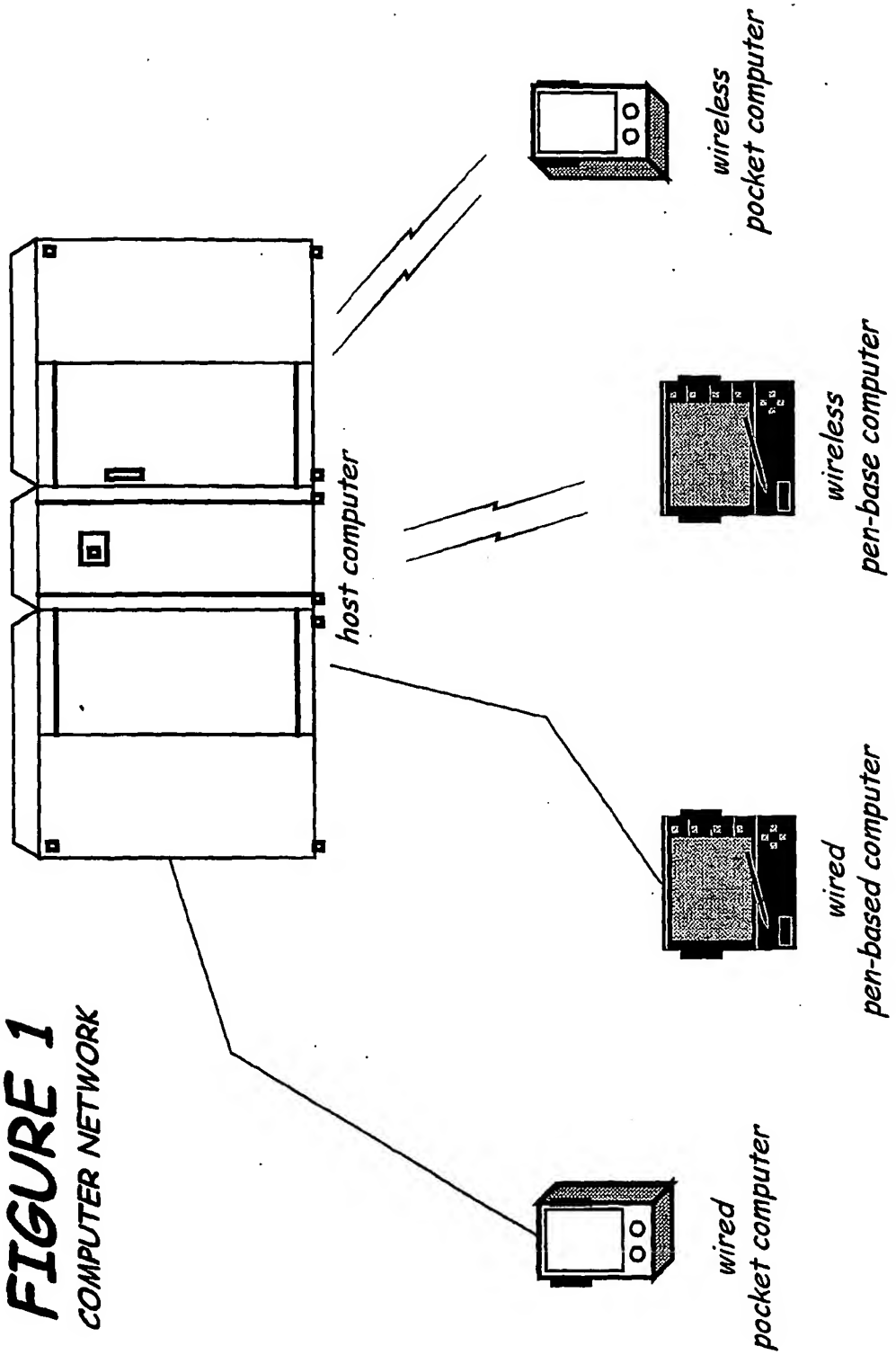


FIGURE 1
COMPUTER NETWORK

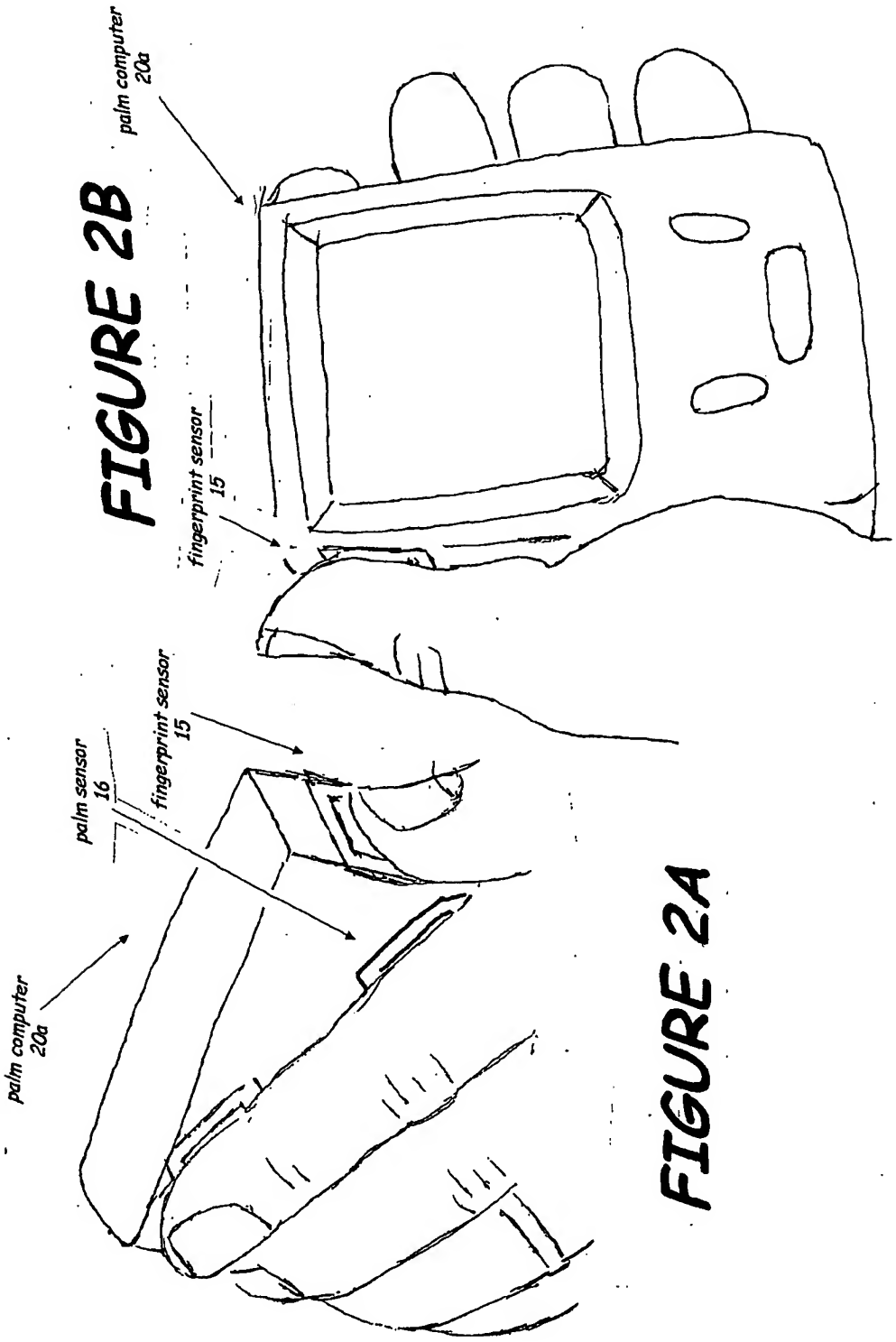


FIGURE 2B

FIGURE 2A

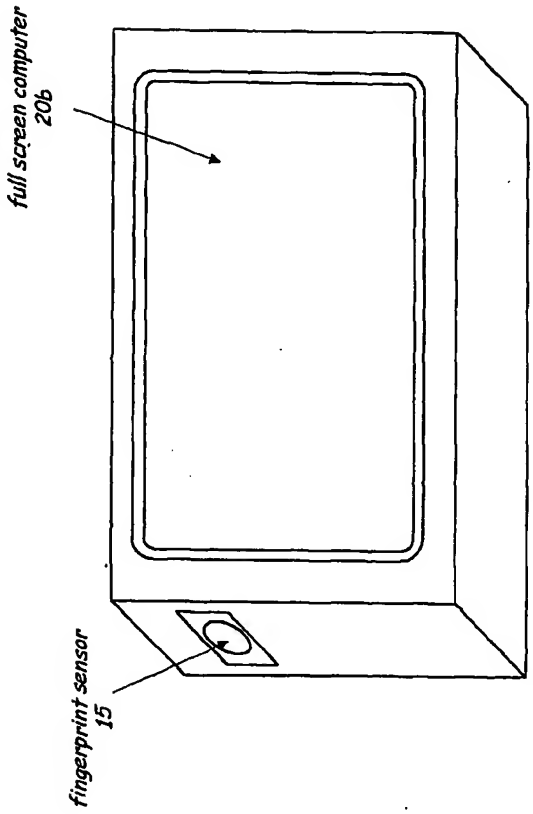


FIGURE 4

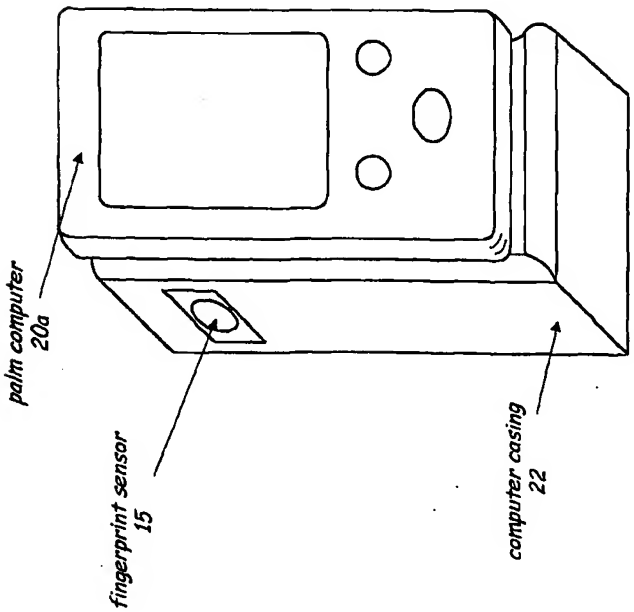


FIGURE 3

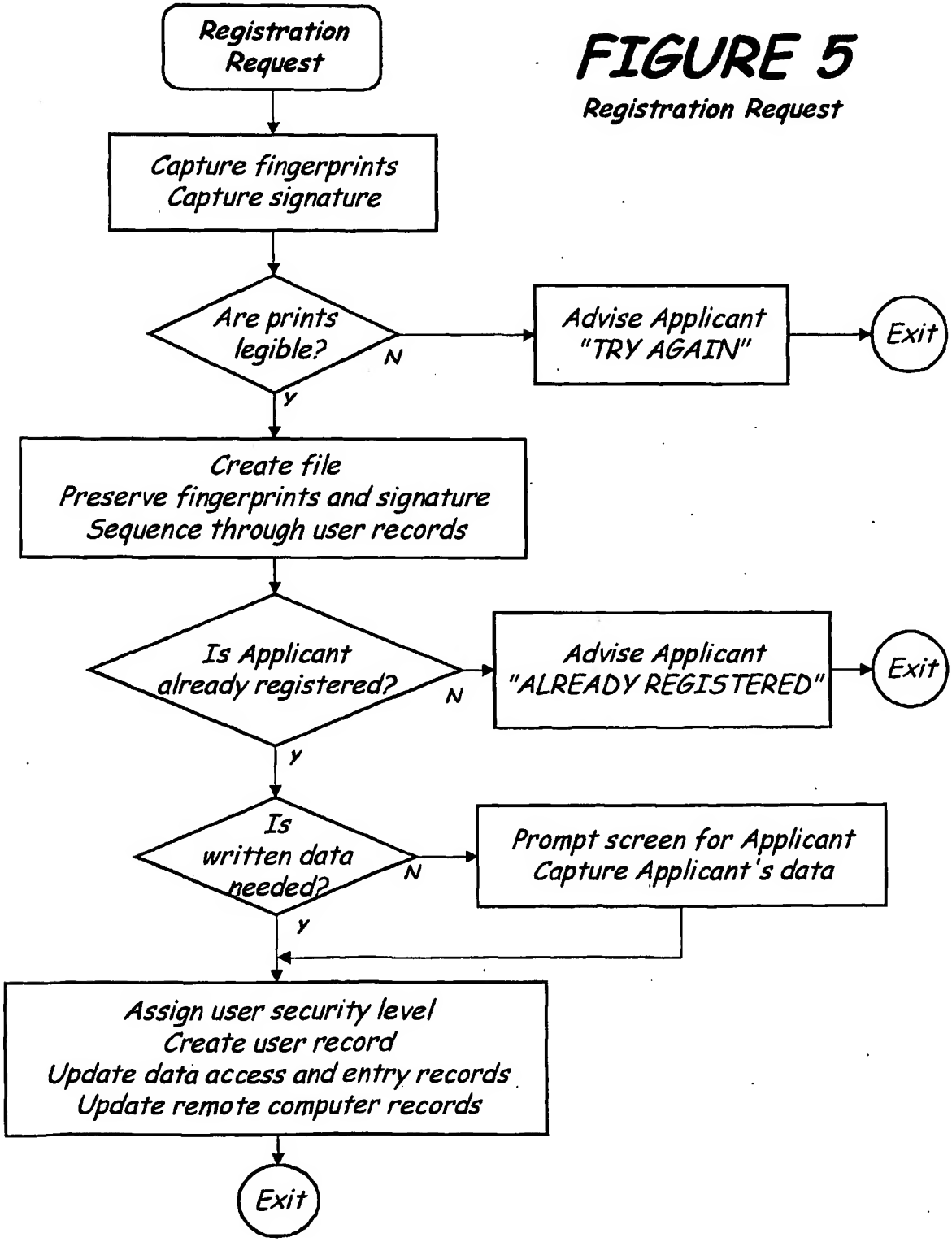
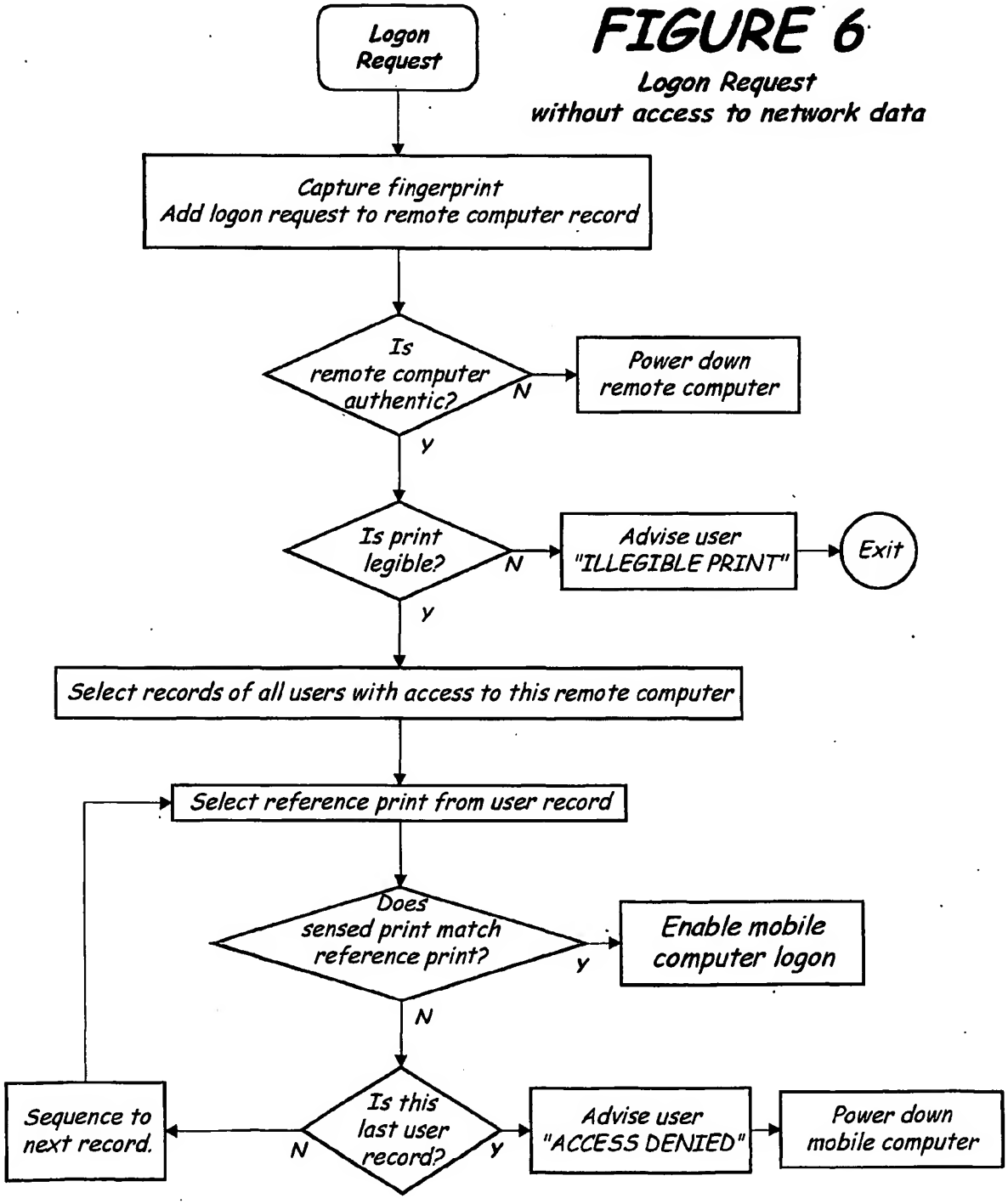


FIGURE 5
Registration Request

FIGURE 6

Logon Request without access to network data



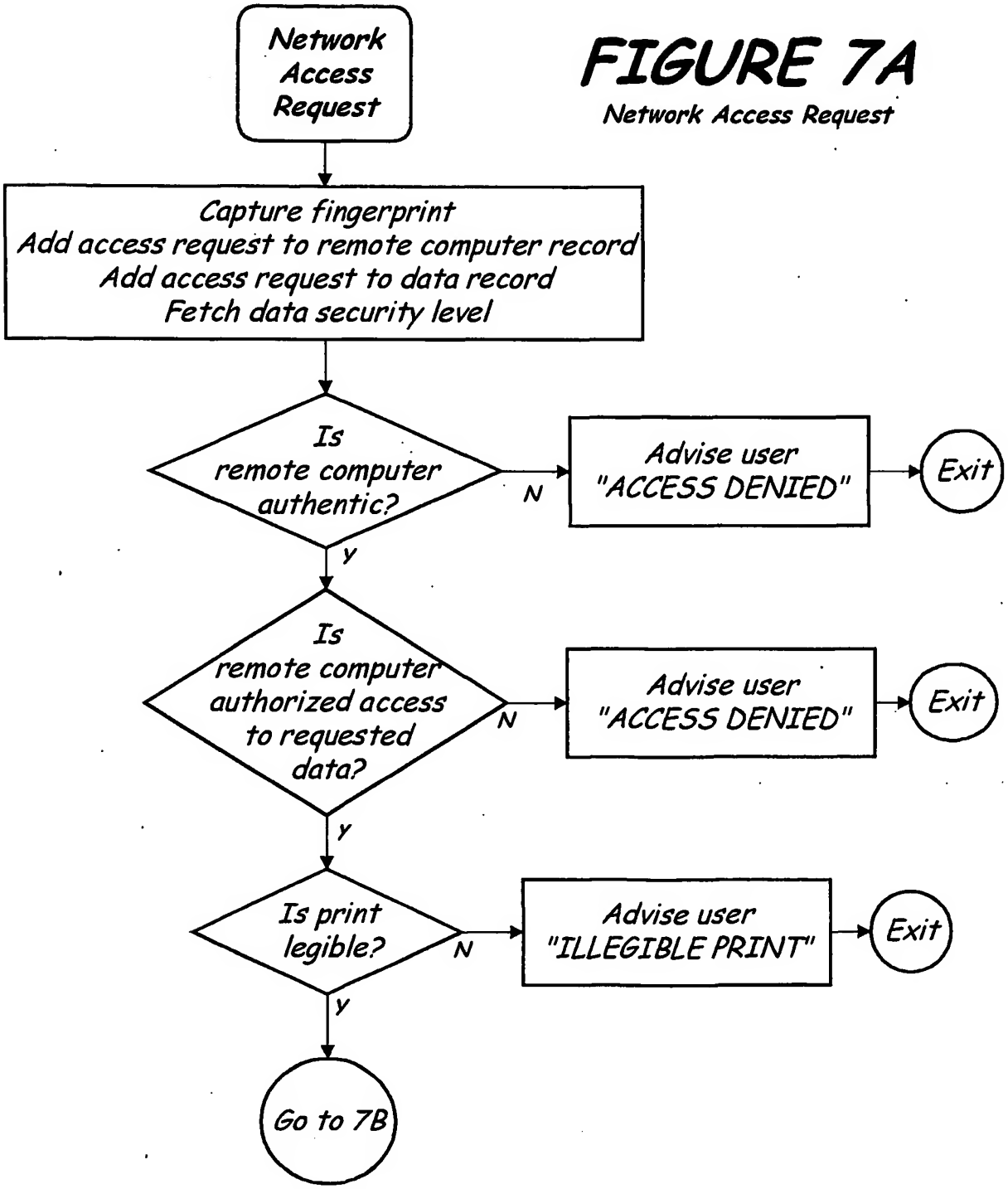


FIGURE 7A
Network Access Request

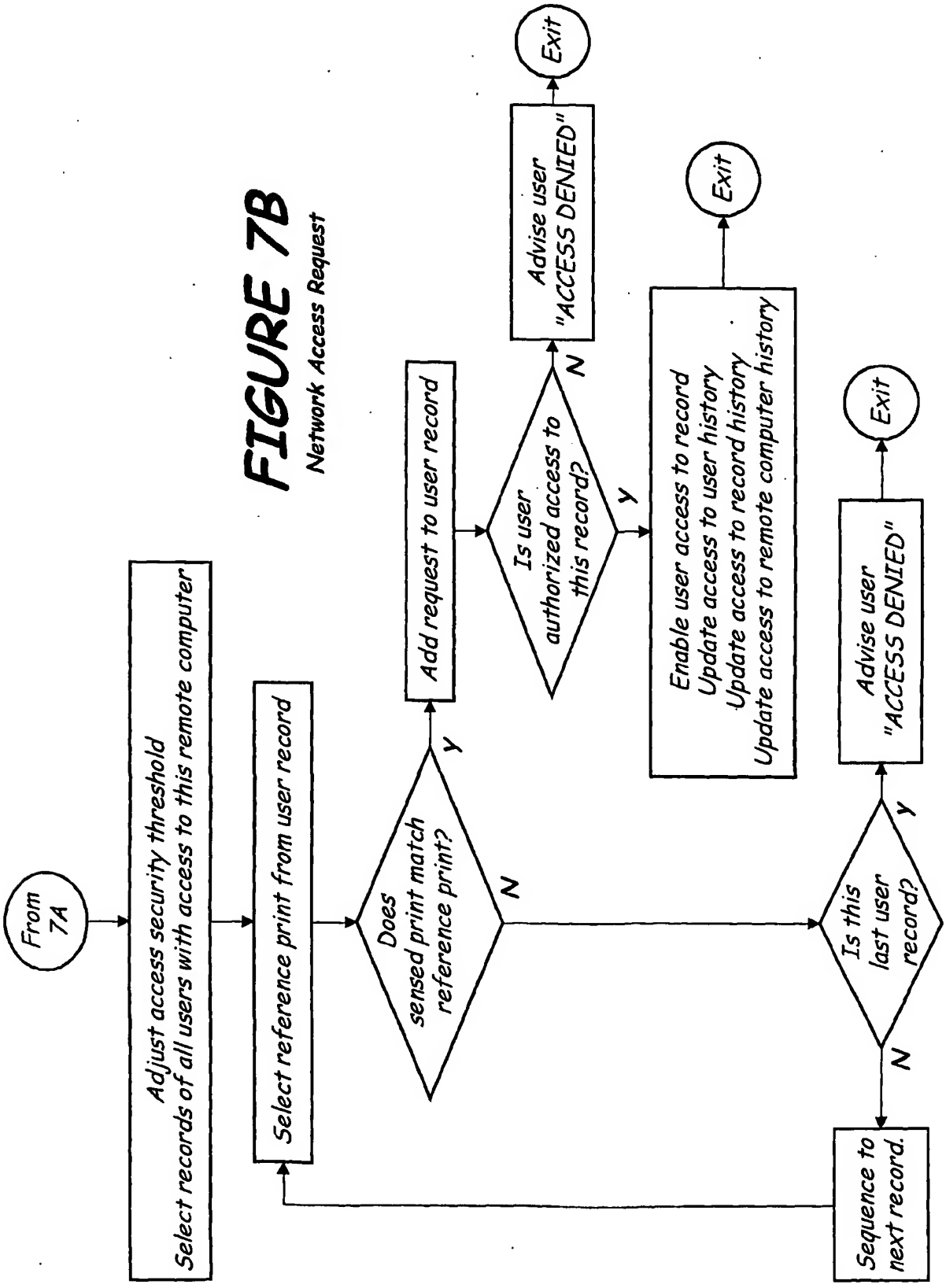


FIGURE 7B
Network Access Request

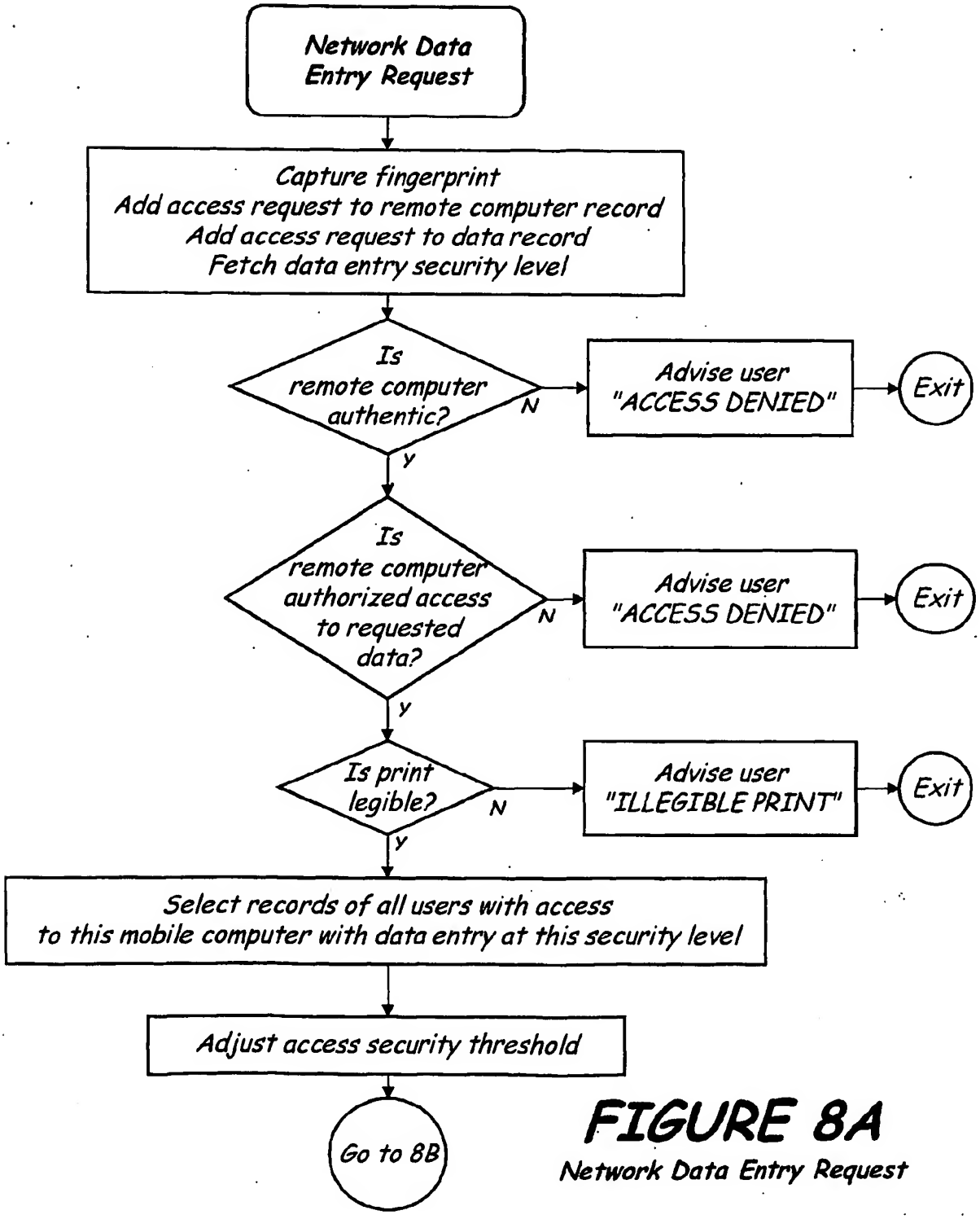
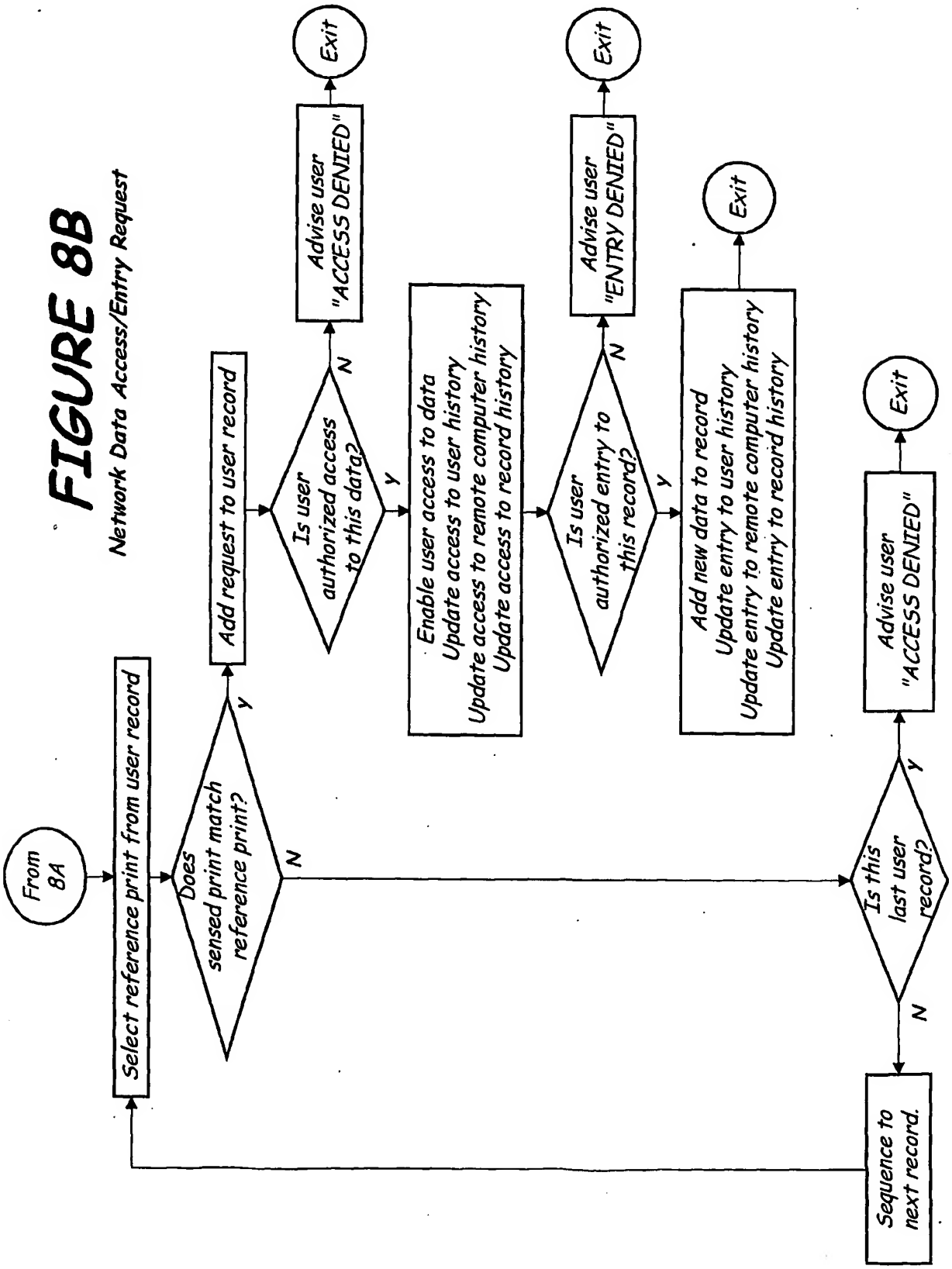


FIGURE 8A
Network Data Entry Request

FIGURE 8B

Network Data Access/Entry Request



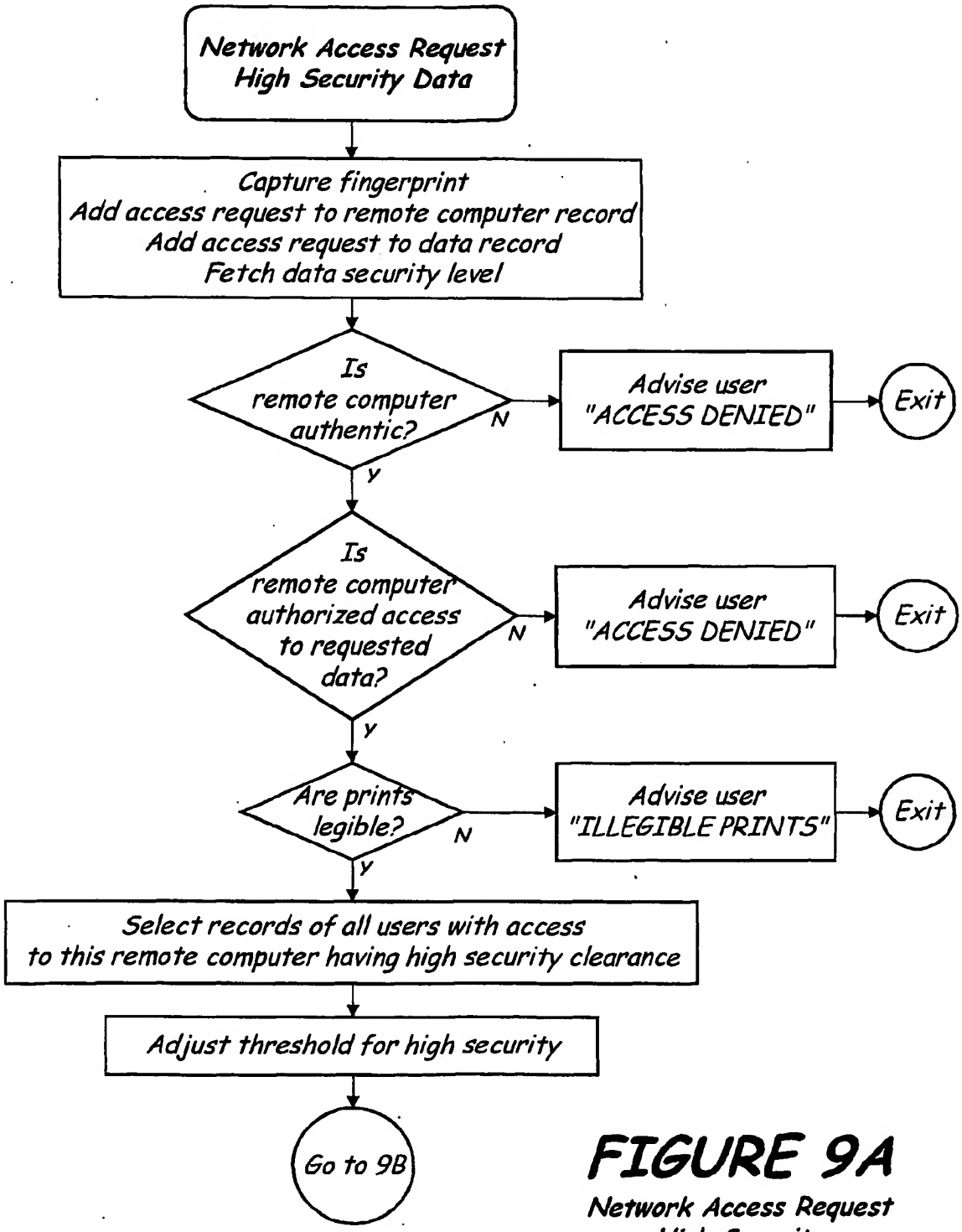


FIGURE 9A
Network Access Request
High Security

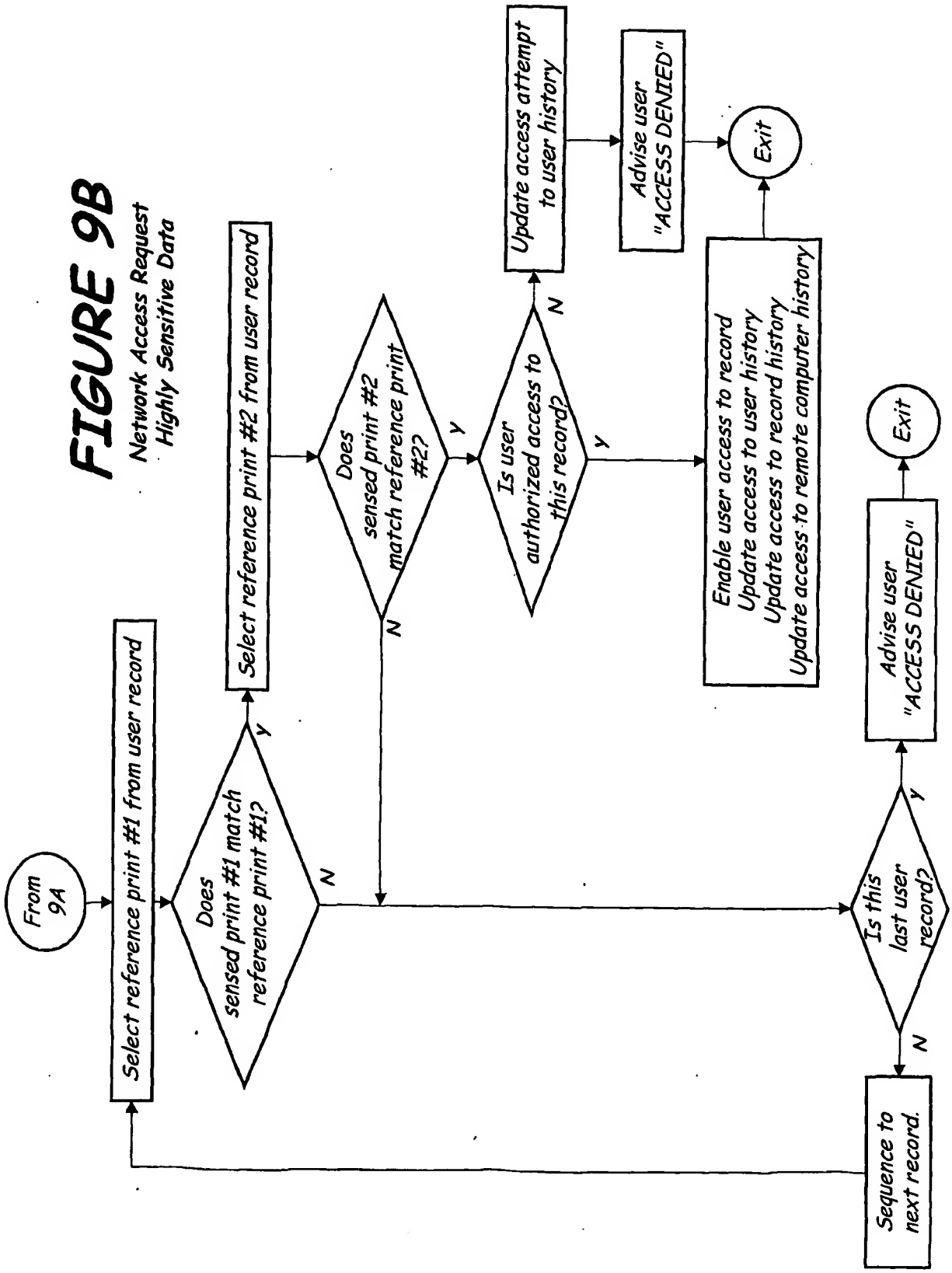


FIGURE 9B

Network Access Request
Highly Sensitive Data

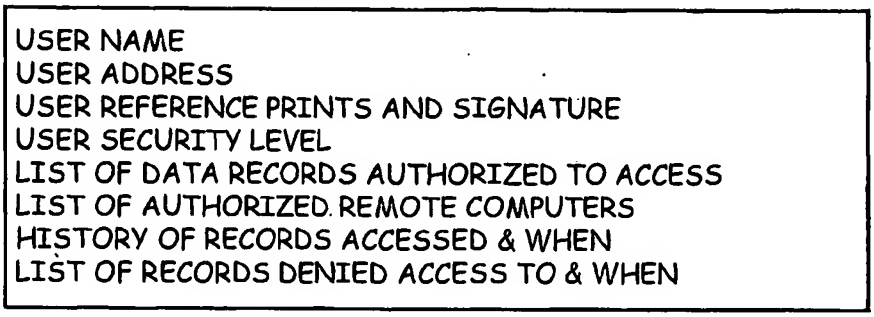


FIGURE 10A
USER RECORD

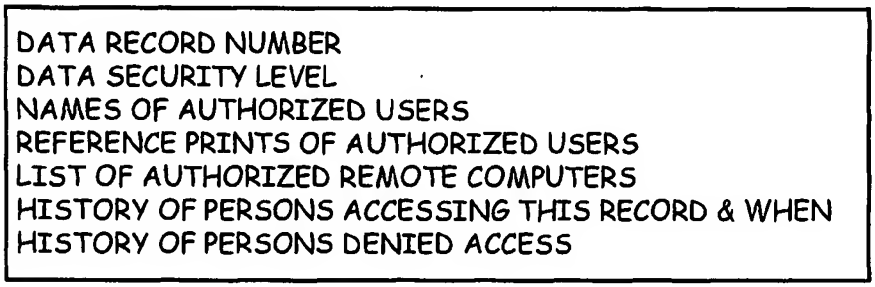


FIGURE 10B
DATA ACCESS RECORD

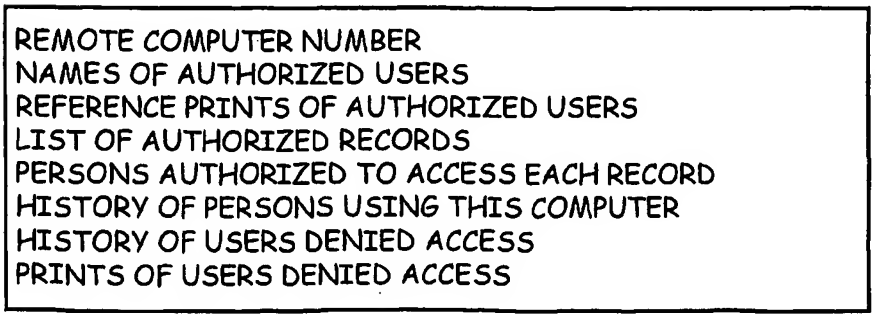


FIGURE 10C
REMOTE COMPUTER RECORD

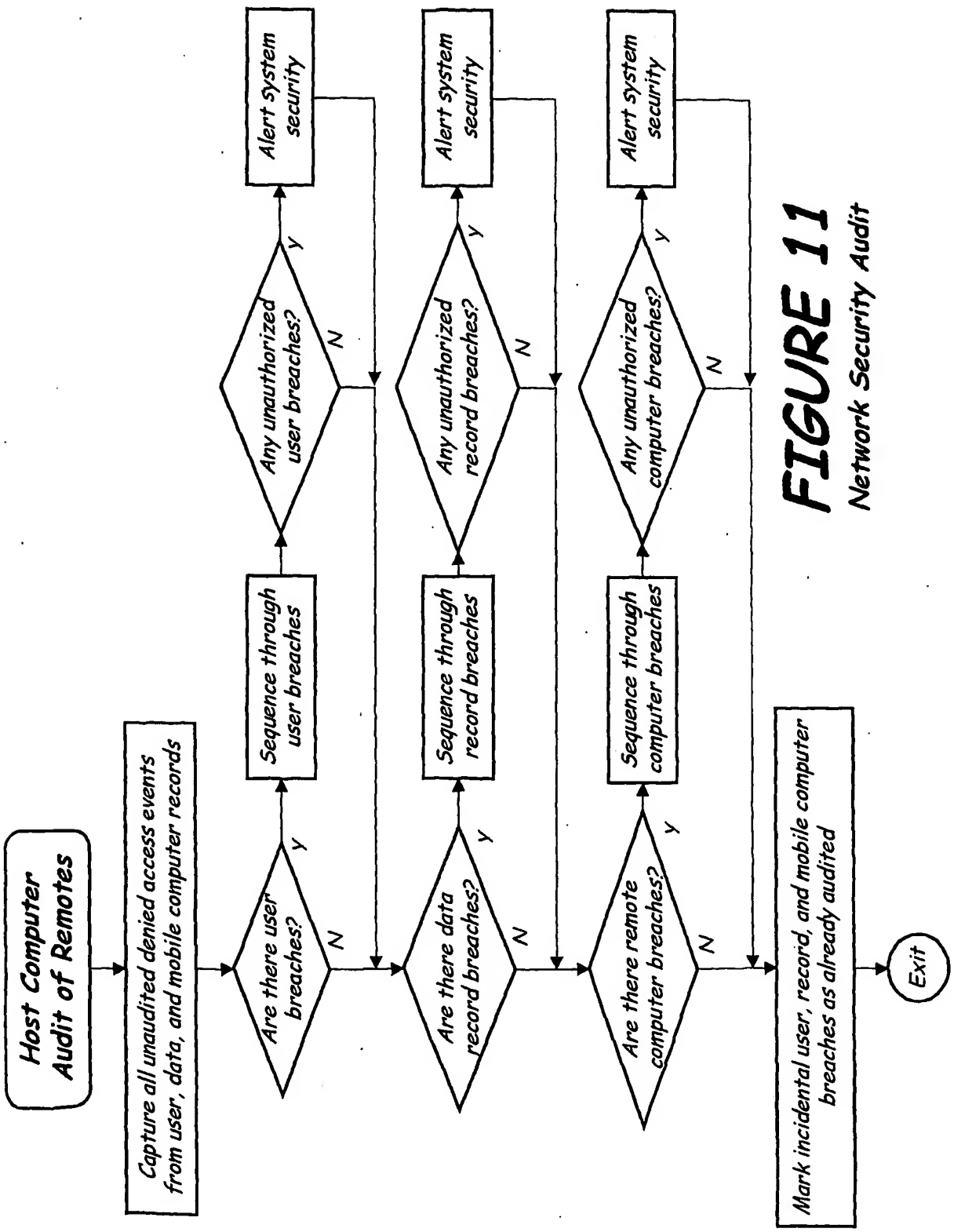


FIGURE 11
Network Security Audit

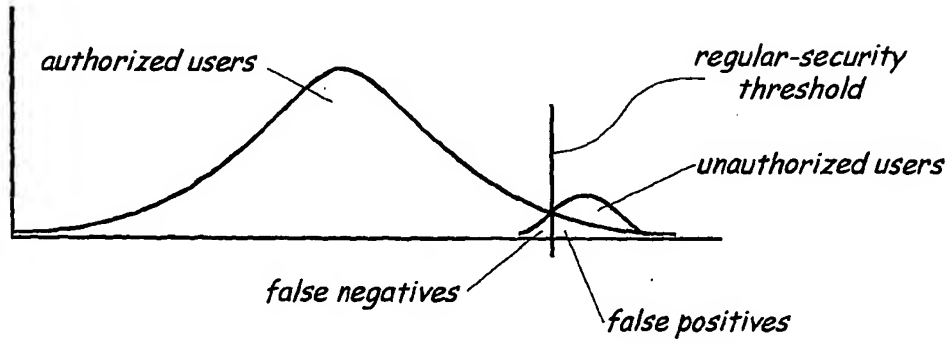


FIGURE 12A
REGULAR SECURITY

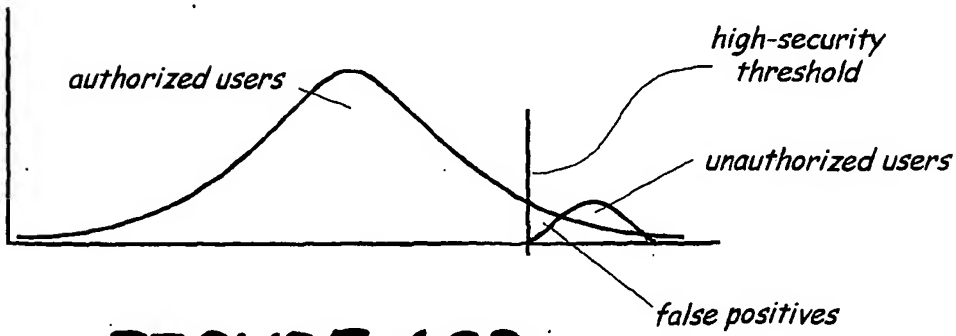


FIGURE 12B
HIGH SECURITY

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/21038

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : H04L 9/00
US CL : 713/186

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 713/186

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EAST database, search terms: "fingerprint near2 authenticat$3"

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6,038,666 A (HSU et al) 14 March 2000 (14.03.2000), see abstract and Fig. 1 and Fig. 3.	1-9
A	US 6,041,410 A (HSU et al) 21 March 2000 (21.03.2000), see abstract	1-9
A	US 6,035,403 A (SUBBIAH et al) 07 March 2000 (07.03.2000), see Fig. 3.	1-9
X,P	US 6,182,221 B1 (HSU et al) 30 January 2001 (30.01.2001), see abstract and Fig. 1 and Fig. 3.	1-9
A,P	US 6,219,793 B1 (LI et al) 17 April 2001 (17.04.2001), see abstract and Fig. 1.	1-9

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
16 October 2001 (16.10.2001)

Date of mailing of the international search report
13 DEC 2001

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703)305-3230

Authorized officer
Albert DeCady
Telephone No. (703) 305-3900

Form PCT/ISA/210 (second sheet) (July 1998)